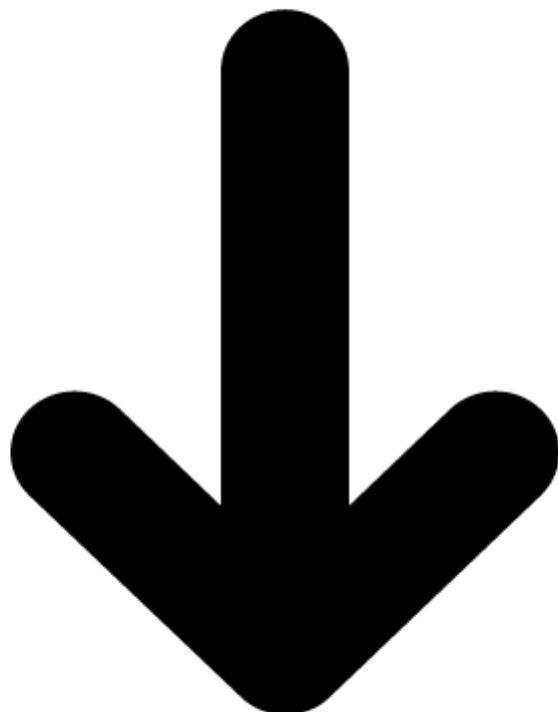


Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata

Nama Kelompok :

- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah



Tahapan 5: Analisis log & pembuatan custom rule

Pada tahapan ini dilakukan analisis terhadap log Suricata untuk mengidentifikasi pola lalu lintas jaringan yang mencurigakan. Berdasarkan hasil analisis tersebut, dibuat beberapa *custom rule* yang bertujuan untuk mendeteksi aktivitas serangan pada jaringan. Aktivitas yang menjadi fokus pada tahap ini meliputi **ping flood**, **scanning menggunakan Nmap**, serta **serangan brute-force login menggunakan Hydra**.

Custom rule dibuat agar sistem IDS mampu memberikan peringatan (alert) ketika terdeteksi pola lalu lintas yang mengindikasikan adanya upaya pengintaian maupun serangan terhadap sistem target. Setiap rule dirancang berdasarkan karakteristik paket dan perilaku jaringan yang dihasilkan oleh masing-masing jenis serangan.

Jenis Aktivitas yang Dideteksi

1. Ping Flood

Ping flood merupakan serangan berbasis ICMP yang dilakukan dengan mengirimkan paket ping secara terus-menerus ke target dalam waktu singkat. Tujuan serangan ini adalah membebani sumber daya jaringan atau host target sehingga dapat menyebabkan penurunan performa atau gangguan layanan. Deteksi ping flood dilakukan dengan memantau lalu lintas ICMP yang masuk ke jaringan target.

2. Scanning Nmap

Scanning Nmap merupakan tahap awal yang umum dilakukan oleh penyerang untuk mengumpulkan informasi mengenai port dan layanan yang aktif pada suatu sistem. Pada pengujian ini, scanning dilakukan menggunakan tiga metode utama, yaitu **TCP SYN Scan (-sS)**, **UDP Scan (-sU)**, dan **NULL Scan (-sN)**.

- **TCP SYN Scan (-sS)**

Merupakan teknik pemindaian port yang mengirimkan paket SYN tanpa menyelesaikan proses koneksi. Metode ini cepat dan sering digunakan karena relatif sulit terdeteksi oleh firewall sederhana.

- **UDP Scan (-sU)**

Digunakan untuk memindai layanan berbasis UDP. Proses scanning ini cenderung lebih lambat karena bergantung pada respons ICMP atau tidak adanya respons dari target.

- **NULL Scan (-sN)**

Dilakukan dengan mengirimkan paket TCP tanpa flag. Teknik ini memanfaatkan perbedaan respons sistem terhadap paket TCP yang tidak memiliki flag untuk menentukan status port.

3. Brute Force Login SSH (Hydra)

Brute-force login merupakan serangan yang dilakukan dengan mencoba banyak kombinasi username dan password secara berulang dalam waktu singkat. Pada

pengujian ini, serangan dilakukan menggunakan tools Hydra yang menargetkan layanan SSH. Pola serangan ditandai dengan banyaknya percobaan koneksi ke port SSH dari satu alamat sumber dalam interval waktu yang singkat.

Tujuan Pembuatan Custom Rule

Pembuatan custom rule pada Suricata bertujuan untuk meningkatkan kemampuan IDS dalam mendeteksi aktivitas mencurigakan yang tidak selalu terdeteksi oleh rule bawaan. Dengan adanya rule khusus ini, sistem dapat memberikan peringatan lebih cepat terhadap aktivitas scanning dan serangan brute-force, sehingga administrator jaringan dapat segera melakukan tindakan mitigasi.

Costum rules dan Analisa log

1. Ping Flood

- Costum rules

```
alert icmp any any -> $HOME_NET any (msg:"CUSTOM - Possible Ping Flood Detected";  
flow:stateless; threshold:type both, track by_src, count 1000, seconds 3; sid:1000002; rev:1;)
```

Rule ini digunakan untuk mendeteksi serangan **Ping Flood**, yaitu pengiriman paket ICMP dalam jumlah sangat besar dalam waktu singkat untuk membanjiri target.

Bagian-bagian rule:

- alert icmp → Suricata memantau trafik ICMP (ping).
- any any -> \$HOME_NET any → serangan bisa berasal dari IP mana saja menuju jaringan internal.
- flow:stateless → pemeriksaan tidak bergantung koneksi, karena ICMP tidak memiliki state.
- threshold:type both, track by_src, count 1000, seconds 3 → jika **satu sumber mengirim 1000 paket dalam 3 detik**, Suricata mengeluarkan alert sebagai indikasi flood.
- msg → pesan yang ditampilkan pada log ketika terdeteksi.
- sid dan rev → identitas rule.

Pengetesan Ping Flood 10.000 paket

```
[kalilinux® Babang-Tamvan)~]$ sudo ping -f -c 10000 192.168.251.3  
PING 192.168.251.3 (192.168.251.3) 56(84) bytes of data.  
--- 192.168.251.3 ping statistics ---  
10000 packets transmitted, 10000 received, 0% packet loss, time 3422ms  
rtt min/avg/max/mdev = 0.135/0.300/1.915/0.091 ms, ipg/ewma 0.342/0.286 ms
```

- Analisa Log

```
ubuntu@ubuntuserver:~$ sudo tail -f /var/log/suricata/fast.log
12/17/2025-10:27:20.978286 [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.1:8 -> 192.168.251.3:0
12/17/2025-10:27:20.978294 [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.1:8 -> 192.168.251.3:0
12/17/2025-10:27:23.912894 [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.1:8 -> 192.168.251.3:0
12/17/2025-10:27:23.912900 [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.3:0 -> 192.168.251.1:0
```

Berdasarkan hasil pemantauan file fast.log, Suricata menghasilkan alert “CUSTOM – Possible Ping Flood Detected” secara berulang. Alert ini menunjukkan bahwa IP 192.168.251.1 mengirimkan paket ICMP Echo Request (type 8) dalam jumlah sangat besar dan cepat menuju host 192.168.251.3, sehingga memenuhi threshold rule (≥ 1000 paket dalam 3 detik).

Target kemudian merespons dengan ICMP Echo Reply, sehingga log juga menampilkan arus balik dari 192.168.251.3 ke 192.168.251.1. Kondisi ini mengindikasikan adanya aktivitas ICMP flooding yang berpotensi membebani jaringan.

2. Scanning Nmap

- costum rules

1. TCP SYN Scan (-sS)

```
alert tcp any any -> $HOME_NET any (flags:S; flow:stateless; msg:"CUSTOM - Possible TCP SYN Scan Detected"; threshold:type both, track by_src, count 10, seconds 5; sid:1001001; rev:1;)
```

Rule ini mendeteksi teknik **TCP SYN scan**, yaitu metode scanning setengah-terbuka yang hanya mengirimkan **paket SYN tanpa melanjutkan koneksi**. Rule akan memicu alert jika **sumber yang sama mengirim ≥ 10 paket SYN dalam 5 detik** ke jaringan internal. Kondisi tersebut menjadi indikator kuat adanya **aktivitas port scanning cepat menggunakan opsi Nmap -sS**.

2. UDP Scan (-sU)

```
alert udp any any -> $HOME_NET any (msg:"CUSTOM - Possible UDP Scan Detected"; flow:stateless; threshold:type both, track by_src, count 15, seconds 5; sid:1001003; rev:2;)
```

Rule ini mendeteksi **percobaan enumerasi layanan UDP**, di mana penyerang mengirim sejumlah paket UDP kosong ke berbagai port untuk melihat respon ICMP unreachable. Suricata akan memberi alert jika terdapat **≥ 15 paket UDP dalam 5 detik dari sumber yang sama**, yang merupakan pola umum **Nmap UDP scanning**.

3. NULL Scan (-sN)

```
alert tcp any any -> $HOME_NET any (msg:"CUSTOM - Possible NULL Scan Detected (-sN)"; flags:0; flow:stateless; threshold:type both, track by_src, count 5, seconds 10; classtype:network-scan; sid:1003001; rev:1;)
```

Rule ini mendeteksi **TCP NULL scan**, yaitu teknik stealth scanning yang mengirim **paket TCP tanpa flag apa pun (flag:0)** untuk mengelabui firewall.

Rule dipicu apabila **≥5 paket tanpa flag dikirim dalam waktu 10 detik**, yang merupakan karakteristik aktivitas **Nmap -sN** untuk identifikasi port open/closed secara silent.

- Pengetesan Nmap dengan server kali linux

```
└─(kalilinux㉿Babang-Tamvan)-[~]
$ nmap -sS 192.168.251.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 17:34 WIB
Nmap scan report for 192.168.251.3 (192.168.251.3)
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

└─(kalilinux㉿Babang-Tamvan)-[~]
$ nmap -sN 192.168.251.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 17:34 WIB
Nmap scan report for 192.168.251.3 (192.168.251.3)
Host is up (0.0026s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds

└─(kalilinux㉿Babang-Tamvan)-[~]
$ nmap -sU 192.168.251.3
```

- Analisa Log yang di hasilkan suricata

```
ubuntu@ubuntuserver:~$ sudo tail -f /var/log/suricata/fast.log
12/17/2025-10:27:20.978286  [**] [1:000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.1:8 -> 192.168.251.3:0
12/17/2025-10:27:20.978294  [**] [1:000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.3:0 -> 192.168.251.1:0
12/17/2025-10:27:23.912894  [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.1:8 -> 192.168.251.3:0
12/17/2025-10:27:23.912900  [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.3:0 -> 192.168.251.1:0
12/17/2025-10:34:40.957483  [**] [1:1001001:1] CUSTOM - Possible TCP SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.251.1:10743 -> 192.168.251.3:554
12/17/2025-10:34:51.385935  [**] [1:1003001:1] CUSTOM - Possible NULL Scan Detected (-sN) [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.251.1:10749 -> 192.168.251.3:993
12/17/2025-10:35:15.678691  [**] [1:1001003:2] CUSTOM - Possible UDP Scan Detected [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.251.1:52913 -> 192.168.251.3:3401
12/17/2025-10:35:21.886858  [**] [1:1001003:2] CUSTOM - Possible UDP Scan Detected [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.251.1:52919 -> 192.168.251.3:45818
12/17/2025-10:35:26.909383  [**] [1:1001003:2] CUSTOM - Possible UDP Scan Detected [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.251.1:52915 -> 192.168.251.3:34577
```

TCP SYN Scan Terdeteksi

Alert ini menunjukkan bahwa sumber 192.168.251.1 mengirim paket TCP dengan flag SYN ke port acak 554 pada host 192.168.251.3. Peningkatan jumlah paket SYN dalam waktu singkat memenuhi threshold rule, sehingga dikategorikan sebagai indikasi **SYN-based port probing menggunakan -sS**.

TCP NULL Scan Terdeteksi

Paket TCP tanpa flag (flags:0) dikirim dari sumber yang sama menuju port 993. Pola ini sesuai karakteristik **Nmap NULL scan (-sN)** untuk mengidentifikasi status port tanpa membuka koneksi. Suricata mengklasifikasikannya sebagai “**Detection of a Network Scan**”.

UDP Scan Terdeteksi

Sumber 192.168.251.1 mengirim paket UDP menuju port 3401 tanpa payload, yang merupakan pola khas **enumerasi UDP (-sU)**. Rule memicu alert setelah jumlah paket melampaui threshold, menandakan percobaan identifikasi layanan UDP.

3. Brute force

- costum Rules

```
alert tcp any any -> $HOME_NET 22 (msg:"SSH BRUTE FORCE ";
flow:to_server,established; content:"SSH-2.0"; nocase; detection_filter:track by_src, count 5,
seconds 30; classtype:attempted-admin; sid:7000001; rev:1;)
```

- **alert tcp any any -> \$HOME_NET 22**
Memantau trafik TCP dari IP mana pun menuju port SSH (22) di jaringan internal.
- **msg:"SSH BRUTE FORCE"**
Pesan alert yang muncul ketika rule terpicu.
- **flow:to_server,established**
Hanya mendeteksi **koneksi yang mengarah ke server dan sudah berhasil terhubung (bukan SYN saja)**.
- **content:"SSH-2.0" nocase**
Mencari **banner protokol SSH**, menandakan sesi login SSH aktif.
- **detection_filter:track by_src, count 5, seconds 30**
Jika 1 sumber IP melakukan ≥ 5 percobaan login dalam 30 detik, dianggap brute-force.
- **classtype:attempted-admin**
Dikategorikan sebagai **upaya mendapatkan akses administrator**.
- **sid:7000001; rev:1**
Nomor identitas rule dan revisinya.

Pengetesan Brute Force

```
GNU nano 8.6
admin
123456
password
target123
root
kuda
dean
```

```
[kalilinux@Babang-Tamvan]~[~/mnt/c/Users/handicap]
$ hydra -l ubuntu -P passlist.txt ssh://192.168.251.3 -t 4 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-17 18:34:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries (l:1/p:7), ~2 tries per task
[DATA] attacking ssh://192.168.251.3:22/
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "admin" - 1 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "123456" - 2 of 7 [child 1] (0/0)
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "password" - 3 of 7 [child 2] (0/0)
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "target123" - 4 of 7 [child 3] (0/0)
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "root" - 5 of 7 [child 3] (0/0)
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "kuda" - 6 of 7 [child 1] (0/0)
[ATTEMPT] target 192.168.251.3 - login "ubuntu" - pass "dean" - 7 of 7 [child 0] (0/0)
[22][ssh] host: 192.168.251.3 login: ubuntu password: dean
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-17 18:34:26
```

Hydra melakukan brute-force terhadap layanan SSH di **192.168.251.3:22** menggunakan username **ubuntu** dan daftar password dari file **passlist.txt**.

Setiap percobaan ditampilkan sebagai **[ATTEMPT]**, menunjukkan login dan password yang sedang diuji. Dari total **7 password** yang dicoba, Hydra berhasil menemukan kecocokan pada password **“dean”**.

Hasil keberhasilan ditandai dengan baris:

[22][ssh] host: 192.168.251.3 login: ubuntu password: dean

yang berarti kredensial valid berhasil ditemukan dan layanan SSH dapat ditembus.

Analisa Hasil Log IDS SURICATA

```
ubuntu@ubuntuserver:~$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for ubuntu:
12/17/2025-10:27:20.978294  [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.3:0 -> 192.168.251.1:0
12/17/2025-10:27:23.912894  [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.1:8 -> 192.168.251.3:0
12/17/2025-10:27:23.912900  [**] [1:1000002:1] CUSTOM - Possible Ping Flood Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.251.3:0 -> 192.168.251.1:0
12/17/2025-10:34:40.957483  [**] [1:1001001:1] CUSTOM - Possible TCP SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.251.1:10743 -> 192.168.251.3:554
12/17/2025-10:34:51.385935  [**] [1:1003001:1] CUSTOM - Possible NULL Scan Detected (-sN) [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.251.1:10749 -> 192.168.251.3:993
12/17/2025-10:35:15.678691  [**] [1:1001003:2] CUSTOM - Possible UDP Scan Detected [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.251.1:52913 -> 192.168.251.3:3401
12/17/2025-10:35:21.886858  [**] [1:1001003:2] CUSTOM - Possible UDP Scan Detected [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.251.1:52919 -> 192.168.251.3:45818
12/17/2025-10:35:26.909383  [**] [1:1001003:2] CUSTOM - Possible UDP Scan Detected [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.251.1:52915 -> 192.168.251.3:34577
12/17/2025-11:30:58.262993  [**] [1:7000001:1] SSH BRUTE FORCE [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.251.1:10774 -> 192.168.251.3:22
12/17/2025-11:30:58.270603  [**] [1:7000001:1] SSH BRUTE FORCE [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.251.1:10720 -> 192.168.251.3:22
```

Berdasarkan hasil pemantauan *fast.log*, Suricata memunculkan alert “**SSH BRUTE FORCE**” dengan klasifikasi **Attempted Administrator Privilege Gain**. Alert ini muncul ketika sumber dengan IP **192.168.251.1** melakukan banyak koneksi TCP berturut-turut menuju port **22** pada host **192.168.251.3**. Aktivitas ini sesuai pola brute-force, yaitu mencoba berbagai password dalam waktu singkat.

Suricata memberikan **Priority 1**, menandakan tingkat ancaman tinggi karena aksi ini berpotensi mendapatkan akses administratif ke sistem target. Dengan demikian, log mengonfirmasi bahwa mekanisme brute-force SSH berhasil terdeteksi sesuai rule yang dibuat.